National Infrastructure Protection Center CyberNotes

Issue #2001-21 *October 22, 2001*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between October 3 and October 19, 2001. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
America Online[1]	Windows 95/98/ME/ NT 4.0/2000	AOL Instant Messenger 4.7	A Denial of Service vulnerability exists if a transferred file contains an unusually long filename.	No workaround or patch available at time of publishing.	AOL Instant Messenger Long Filename Denial of Service	Low	Bug discussed in newsgroups and websites.
Andries Brouwer[2]	Unix	util-linux 2.11h, 2.11i, 2.11k, 2.11l	A vulnerability exists when the number of users that access the system is regulated by 'pam_limits', which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Util-Linux Login Pam Privilege Elevation	Medium	Bug discussed in newsgroups and websites.

[1] Bugtraq, October 6, 2001.

[2] Bugtraq, October 8, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Apple[3]	MacOS	Claris 2.0	A buffer overflow vulnerability exists when an e-mail is received with an unusually long filename attachment, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Apple Claris Emailer Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Apple[4]	MacOS X 10.0-10.1	MacOS X 10.0-10.1	A vulnerability exists because superuser privileges are not dropped when applications are spawned in the 'Recent Items' list and the 'Services' menu, which could let a malicious user execute arbitrary code with root privileges.	No workaround or patch available at time of publishing.	MacOS X NetInfo Manager Privilege Escalation	**High**	Bug discussed in newsgroups and websites. There is no exploit code required. Vulnerability has appeared in the press and other public media.
Atomz Corporation[5]	Multiple	Enterprise Search 1.0, Express Search 1.0, Prime Search 1.0	A vulnerability exists because the search engines do not filter HTML image tags from search queries, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Search Engine Cross-site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
Cerulean Studios[6]	Windows 98/98/ME/ NT 4.0/2000	Trillian 0.6351	A Denial of Service vulnerability exists if an AIM instant message contains an unusual number of characters.	No workaround or patch available at time of publishing.	Trillian Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems[7]	Multiple	CatOS 4.5(1), IOS 11.1-11.3.11b, 12.0(5.1)XP, 12.0.19, 12.1	A Denial of Service vulnerability exists due to the way Cisco routers handle the Cisco Discovery Protocol (CDP).	Update available at: http://www.cisco.com	Cisco Discovery Protocol Neighbor Announcement Denial of Service	Low	Bug discussed in newsgroups and websites.
Cisco Systems[8]	Multiple	PIX Firewall Manager 4.3(2)g	A vulnerability exists in the PIX Firewall Manager (PFM) software because the administrative password is stored in plaintext, which could let a malicious user connect to the PIX Firewall and make configuration changes.	**Workaround:** Cisco recommends replacing the PIX Firewall Manager software with PIX Device Manager.	PIX Firewall Manager Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[3] Bugtraq, October 19, 2001.
[4] VulnWatch, October 18, 2001.
[5] Bugtraq, October 11, 2001.
[6] Bugtraq, October 3, 2001.
[7] VulnWatch, October 9, 2001.
[8] Bugtraq, October 11, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Citrix[9]	Windows NT/2000	MetaFrame XP, MetaFrame for Windows 2000 1.8, MetaFrame for Windows NT 4.0 TSE 1.8	A remote Denial of Service vulnerability exists due to improper handling of the multiple sessions.	Hotfix available at: http://www.citrix.com/support	MetaFrame Multiple Sessions Denial of Service CVE Name: CAN-2001-0716	Low	Bug discussed in newsgroups and websites.
Digex[10]	Unix	Looking Glass 1.0	A vulnerability exists due to insufficient validation of input, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Looking Glass Perl Script Neighbor Information Gathering	Medium	Bug discussed in newsgroups and websites.
Francisco Burzi[11]	Unix	PostNuke 0.62-0.64	A vulnerability exists in the 'article.php' and 'mainfile2.php' components due to the failure to filter inappropriate characters from variables that can be passed to the programs, which could let a remote malicious user bypass password checking and assume the identity of a specified user.	Upgrade available at: http://prdownloads.sourceforge.net/post-nuke/64Mutant_Fix_article.zip	PostNuke Unauthenticated User Login	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
gFTP [12]	Unix	gFTP 2.0.6a	A vulnerability exists because the password is displayed in plain text within the log window, which could let a remote malicious user gain elevated privileges.	Upgrade available at: http://security.debian.org/dists/stable/updates/	gFTP On-Screen Plaintext Password	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Hewlett Packard[13]	Unix	HP-UX 11.20	A vulnerability exists in the 'geteuid' system, which could let a malicious user gain elevated privileges.	Upgrade available at: PHSS_25454 http://itrc.hp.com	HP-UX GetEUID	Medium	Bug discussed in newsgroups and websites.
ht://Dig Group[14, 15, 16]	Unix	ht://Dig 3.20b2, 3.20b3, 3.1.5, 1.5-7	A remote Denial of Service vulnerability exists due to the fact that it is possible to use command line arguments from the web interface. This vulnerability could also let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.htdig.org/files/snapshots/ **Conectiva Linux:** ftp://atualizacoes.conectiva.com.br/ **Caldera:** ftp://ftp.caldera.com/pub/updates/OpenLinux/3.1/Server/current/RPMS **Debian:** http://security.debian.org/dists/stable/updates	ht://Dig Remote Denial of Service/File Disclosure	Low/ Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.

[9] Internet Security Systems Security Advisory, October 6, 2001.
[10] Bugtraq, October 18, 2001.
[11] Bugtraq, October 13, 2001.
[12] Debian Security Advisory, DSA 084-1, October 18, 2001.
[13] Hewlett-Packard Company Security Bulletin, HPSBUX0110-171, October 19, 2001.
[14] Conectiva Linux Security Announcement, CLA-2001:429, October 10, 2001.
[15] Caldera International, Inc. Security Advisory, CSSA-2001-035.0, October 10, 2001.
[16] Debian Security Advisory, DSA 080-1, October 17, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hylafax[17] ***Exploit code released***[18]	**Unix**	**Hylafax 4.1**	**A format string vulnerability exists because input isn't sufficiently sanitized when the hostname is entered, which could let a malicious user gain elevated privileges and execute arbitrary code.**	**No workaround or patch available at time of publishing.**	**Hylafax Hostname Format String**	**High**	**Bug discussed in newsgroups and websites.** ***Exploit code has been published.***
IPSwitch[19]	Windows NT 4.0/2000	IMail 7.0.4 and prior	Multiple security vulnerabilities exist which include e-mail hijacking, mailbox disclosure, attachment information leak, weak session ID, and a Denial of Service. These vulnerabilities could let a malicious user gain sensitive information or cause a Denial of Service.	Hotfix available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/IM704HF1.exe	IMail Multiple Security Vulnerabilities	Low/ Medium	Bug discussed in newsgroups and websites. There is no exploit code required and some can be exploited with a web browser.
IPSwitch[20]	Windows NT 4.0/2000	IMail 7.0.4 and prior	A buffer overflow vulnerability exists in the Web Calendaring feature due to improper bounds checking, which could let a malicious user execute arbitrary code.	Hotfix available at: ftp://ftp.ipswitch.com/Ipswitch/Product_Support/IMail/imail1704.exe	IMail Web Calendar Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Linus Torvalds[21]	Unix	Linux kernel 2.4-2.4.11	A vulnerability exists in the Netfilter functions of the Linux Kernel, which could let a remote malicious user gain access to sensitive systems.	**Workaround:** Use the latest version of iptables (1.2.3) from: http://netfilter.samba.org	Linux Kernel MAC Module Filtering Bypassing	Medium	Bug discussed in newsgroups and websites.
Microsoft[22]	Windows ME	Windows ME	A Denial of Service vulnerability exists in the Simple Service Discovery Protocol (SSDP) when a string of arbitrary characters is sent.	Unofficial workaround (Bugtraq): Disable Universal Plug and Play (UPnP).	Windows ME Simple Service Discovery Protocol Denial of Service	Low	Bug discussed in newsgroups and websites.
Microsoft[23]	Windows NT 4.0/2000	Windows 2000 Advanced Server SP1&SP2, Windows 2000 Datacenter Server SP1&SP2, Windows 2000 Server SP1&SP2, Windows NT Terminal Server	A remote Denial of Service vulnerability exists in the implementation of the Remote Data Protocol (RDP) because it does not correctly handle a particular series of data packets.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/security/bulletin/ms01-052.asp	Windows Terminal Server Service RDP Denial of Service	Low	Bug discussed in newsgroups and websites.

[17] Bugtraq, September 24, 2001.
[18] Securiteam, October 15, 2001.
[19] Securiteam, October 15, 2001.
[20] Defcom Labs Advisory, def-2001-29, October 12, 2001.
[21] Netservers Security Advisory, October 8, 2001.
[22] Bugtraq, October 17, 2001.
[23] Microsoft Security Bulletin, MS01-052, October 18, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[24]	Windows 95/98/ME/ NT 4.0/2000	Internet Explorer 5.01, 5.5, 6.0	Three vulnerabilities exist: the first involves how IE handles URLs that include dotless IP addresses, which could let a malicious user run the site with fewer security restrictions (this does not affect IE 6.0); the second vulnerability involves how IE handles URLs that specify third-party sites, which could let a malicious user send a user to a third-party web site and send commands to it in the guise of the user; and the third vulnerability is a new variant of a vulnerability discussed in Microsoft Security Bulletin MS01-015 (located at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-015.asp), affecting how Telnet sessions are invoked via IE, which could let a malicious user write files onto a user's computer via Telnet.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-051.asp	Internet Explorer HTTP Request Encoding, Zone Spoofing, and Telnet Invocation CVE Name: CAN-2001-0664, CAN-2001-0665, CAN-2001-0667	Medium	Bug discussed in newsgroups and websites.
Mountain Network Systems Inc.[25]	Multiple	WebCart 8.4	A vulnerability exists in the 'webcart.cgi' script, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	WebCart Command Execution	**High**	Bug discussed in newsgroups and websites. This can be exploited with a web browser.
Multiple Vendors[26]	Unix	Linux kernel 2.2- 2.2.19, 2.4-2.4.9	A Denial of Service vulnerability exists when a malicious user creates a long chain of symbolically linked files.	Upgrade available at: ftp://ftp.us.kernel.org/pub/linux/kernel/v2.4/linux-2.4.12.tar.gz	Linux Deep Symbolic Link Denial of Service	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Multiple Vendors[27, 28, 29]	Unix	Linux kernel 2.2- 2.2.19, 2.4.2, 2.4.9	A vulnerability exists in the 'exec()' implementation, which could let a malicious user gain access to the root account.	**Caldera:** ftp://ftp.caldera.com/pub/updates/ **EnGarde Linux**: ftp://ftp.engardelinux.org/pub/engarde/stable/updates/ **RedHat:** ftp://updates.redhat.com/	Linux Ptrace/Setuid Exec	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[24] Microsoft Security Bulletin, MS01-051, October 10, 2001.
[25] Bugtraq, October 19, 2001.
[26] Bugtraq, October 18, 2001.
[27] Caldera Security Advisory, CSSA-2001-036.0, October 18, 2001.
[28] EnGarde Secure Linux Security Advisory, ESA-20011019-02, October 19, 2001.
[29] Red Hat Security Advisory, RHSA-2001:129-05, October 18, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Novell[30]	Windows 2000	Groupwise 6.0, Groupwise Enhancement Pack 5.5	A vulnerability exists in the WebAccess system, which could let a remote malicious user view sensitive information.	Upgrade available at: http://support.novell.com/servlet/tidfinder/2960443	Novell Groupwise Arbitrary File Retrieval	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser. Vulnerability has appeared in the press and other public media.
OpenBSD[31]	Unix	OpenBSD 2.0-2.9	A vulnerability exists which could let a malicious user sent signals to processes running on the system belonging to other users.	No workaround or patch available at time of publishing.	OpenBSD Connected Socket Ownership	Low	Bug discussed in newsgroups and websites.
OpenSSH[32] ***Other Vendors provide patches***[33, 34, 35, 36]	**Unix**	**OpenSSH 2.5-2.5.2, 2.9**	**A vulnerability exists when two keys of different types appear successively in the '.authorized_keys2' file, which could let a remote malicious user bypass some access control and log in from unauthorized hosts.**	**Upgrade available at:** **ftp://ftp.openbsd.org/pub/OpenBSD/OpenSSH/openssh-2.9.9.tgz** ***RedHat:*** **ftp://updates.redhat.com** ***LinuxMandrake:*** **http://www.linux-mandrake.com/en/ftp.php3** ***Trustix:*** **http://www.trustix.net/pub/Trustix/updates/** ***Immunix:*** **http://immunix.org/ImmunixOS/**	**OpenSSH Key Based Source IP Access Control Bypass**	**Medium**	**Bug discussed in newsgroups and websites. There is no exploit code required.**
Oracle Corporation[37]	Windows NT 4.0/2000, Unix	Oracle9iAS Web Cache 2.01.0	A buffer overflow vulnerability exists when a malicious URL is submitted, which could let a malicious user execute arbitrary code.	Patch available at: http://metalink.oracle.com	Oracle9iAS Web Cache Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
phpBB Group[38]	Multiple	phpBB 1.4.2	A vulnerability exists in phpBB, which makes it possible for a malicious user to remotely manipulate the logic of SQL queries. As a result, it may be possible for attackers to force malicious database operations.	No workaround or patch available at time of publishing.	phpBB 'bb_memberlist.php' Remote SQL Query Manipulation	Medium	Bug discussed in newsgroups and websites. This can be exploited with a web browser.

[30] Foundstone Advisory, FS-101501-20-GWSE, October 15, 2001.
[31] Securiteam, October 8, 2001.
[32] OpenSSH Security Advisory, September 26, 2001.
[33] Red Hat Security Advisory, RHSA-2001:114-04, October 16, 2001.
[34] Mandrake Linux Security Update Advisory, MDKSA-2001:081, October 16, 2001.
[35] Trustix Secure Linux Security Advisory, TSLSA-2001-0023, October 17, 2001.
[36] Immunix OS Security Advisory, MNX-2001-70-034-01, October 18, 2001.
[37] Defcom Labs Advisory, def-2001-30, October 18, 2001.
[38] Bugtraq, October 8, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Progress Software[39]	Windows NT 4.0/2000, Unix	Progress Database 8.3D, 9.1C	Multiple vulnerabilities exist: several buffer overflow vulnerabilities exist due to insufficient bounds checking; and an input validation vulnerability exists in 'jvmStart', which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Progress Database Multiple Buffer Overflow and Input Validation	**High**	Bug discussed in newsgroups and websites.
Progress Software[40]	Windows NT 4.0/2000, Unix	Progress Database 8.3D, 9.1C	A buffer overflow vulnerability exists in the way long entries are handled in the 'protermcap' file, which could let a malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Progress Database Malicious ProTermCap File Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sambar Development Team[41]	Unix	HP CIFS/ 9000 Server A.01.05, A.01.06; Samba 2.0.5-2.2.0	A vulnerability exists because the 'smb' daemon does not sufficiently check NetBIOS name input, which could let a remote malicious user execute arbitrary code.	Contact your vendor for upgrade.	Samba Remote Arbitrary File Creation	**High**	Bug discussed in newsgroups and websites. Exploits and an exploit script have been published.
SCO[42]	Unix	UnixWare 7.1	A buffer overflow exists in 'sgid-lps' which could let a malicious user gain root privileges.	Update available at: http://www.sco.com	UnixWare LPsystem Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Snes9x. com[43]	Unix	Snes9x.com 1.3.4, 1.3.7	A buffer overflow vulnerability exists due to improper bounds checking of rom names, which could let a malicious user execute arbitrary code.	Upgrade available at: http://www.snes9x.com/	Snes9x Local Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Symantec Corporation[44]	Multiple	LiveUpdate 1.4, 1.5	A vulnerability exists because Cryptography (Digital Signatures, Public Keys or Certificates) are not used when performing LiveUpdates, which could let a remote malicious user send hostile code.	Update available at: http://www.symantec.com/techsupp/files/lu/lu.html	LiveUpdate Host Verification	Medium	Bug discussed in newsgroups and websites. Exploit has been published. Vulnerability has appeared in the press and other public media.
Trend Micro, Incorporated[45]	Windows 95/98/ME/ NT 4.0/2000	Trend Micro 3.53, Virus Buster Corporate Edition 3.53	A vulnerability exists due to a flaw in the implementation of the 'hotdownload' virtual directory, which could let a remote malicious user obtain sensitive information.	Patch available at: http://www.trendmicro.co.jp/esolution/solutionDetail.asp?solutionID=3182	Trend Micro OfficeScan Virtual Directory Disclosure	Medium	Bug discussed in newsgroups and websites.

[39] Bugtraq, October 5, 2001.
[40] Bugtraq, October 8, 2001.
[41] SecurityFocus, October 16, 2001.
[42] Securiteam, October 8, 2001.
[43] Bugtraq, October 16, 2001.
[44] Phenoelit Advisory #0815, October 5, 2001.
[45] SNS Advisory No.44, October 16, 2001.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
TYPSoft[46]	Windows 95/98/ME/ NT 4.0/2000	TYPSoft FTP Server 0.95	A Denial of Service vulnerability exists when a malicious argument string is submitted using either 'RETR' or 'STOR' commands.	No workaround or patch available at time of publishing.	TYPSoft FTP 'RETR' and 'STOR' Denial of Service Vulnerability	Low	Bug discussed in newsgroups and websites. Exploit script has been published.
Zope Project[47, 48]	Unix	Zope 2.2.0-2.2.5	A vulnerability exists in 'fmt,' which could let a malicious user to gain unauthorized access to resources on the host.	Upgrade available at: http://www.zope.org/Products /Zope/Hotfix_2001-09-28/ **RedHat:** ftp://updates.redhat.com/ **Mandrake Linux:** http://www.linux-mandrake.com/en/ftp.php3	Zope DTML Format Method Checking	Medium	Bug discussed in newsgroups and websites.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between October 4 and October 18, 2001, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 12 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 18, 2001	Linuxptrace-exp.tgz	Script which exploits the Linux Ptrace/Setuid Exec vulnerability.

[46] Asguard Labs Advisory, October 4, 2001.
[47] Red Hat Security Advisory, RHSA-2001:115-05, October 10, 2001.
[48] Mandrake Linux Security Update Advisory, MDKSA-2001:080, October 15, 2001.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
October 18, 2001	Mklink.sh	Script which exploits the Linux Deep Symbolic Link Denial of Service vulnerability.
October 18, 2001	Webcache.pl	Perl script which exploits the Oracle9iAS Web Cache Buffer Overflow vulnerability.
October 17, 2001	Dcetest-1.2.tar.gz	A tool which probes a Windows machine over TCP port 135 and can be very useful once inside a DMZ to fingerprint Windows machines on the network.
October 17, 2001	Ethereal-0.8.20.tar.gz	A GTK+-based network protocol analyzer, or sniffer, that lets you capture and interactively browse the contents of network frames.
October 17, 2001	Samba.sh	Script which exploits the Samba Remote Arbitrary File Creation vulnerability.
October 17, 2001	Sharefuzz1.0.tar.gz	A shared library that automatically detects environment variable overflows in Unix systems and can be used as a reverse engineering tool.
October 17, 2001	Spike-v1.8.tar.gz	An easy to use generic protocol API that helps reverse engineer new and unknown network protocols, which features several working examples.
October 16, 2001	Samba-exp.sh	Script which exploits the Samba Remote Arbitrary File Creation vulnerability.
October 10, 2001	Formatstring-1.2.tar.gz	Exploiting Format String Vulnerabilities describes techniques and examples for exploiting format string vulnerabilities.
October 10, 2001	Irs15.exe	IP Restrictions Scanner (IRS) is a Windows NT/2000 tool that finds out which network restrictions have been set for a particular service on a host. It combines "ARP Poisoning" and "Half-Scan" techniques and tries totally spoofed TCP connections to the selected port of the target.
October 4, 2001	**Typ095dos.pl**	**Perl script which exploits the TYPSoft FTP 'RETR' and 'STOR' Denial of Service Vulnerability**

Trends

Probes/Scans:

- **CERT/CC continues to observe increased network reconnaissance activity and a significant increase in the number of generalized port scans of hosts.**

Other:

- The FBI's computer crime division is warning Americans to expect an increase in cyber protests and "hacktivism" in the wake of the U.S. response to the Sept. 11 terrorist attacks. For more information, see “Cyber Protest: The Threat to the U.S. Information Infrastructure,” located at: http://www.nipc.gov/cyberprotests.pdf.
- The Redesi worm disguises itself as a security patch for Microsoft products and is set to trigger on November 11, 2001. For more information, see Virus Section.
- **The National Infrastructure Protection Center (NIPC) continues to observe hacking activity targeting the e-commerce or e-finance/banking industry. For more information, see NIPC ADVISORY 01-023 located at: http://www.nipc.gov/warnings/advisories/2001/01-023.htm. The most prevalent exploit being used to gain access to targeted systems is the Unicode vulnerability found in the Microsoft Internet Information Services (IIS) web server software, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS00-086.asp**
- **The National Infrastructure Protection Center expects to see an upswing in incidents as a result of the tragic events of September 11, 2001. For more information, see NIPC ADVISORY 01-020, available at http://www.nipc.gov/warnings/advisories/2001/01-020.htm.**

Viruses

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication**. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available**. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported during the latest three months), and approximate date first found. During this month, a number of anti-virus vendors have included information on Trojan Horses and Worms. Following this table are descriptions of new viruses and updated versions discovered in the last two weeks. NOTE: At times, viruses may contain names or content that may be considered offensive.

Ranking	Common Name	Type of Code	Trends	Date
1	W32/Nimda	File, Worm	Stable	September 2001
2	W32/SirCam	Worm	Stable	July 2001
3	W32/Magistr-(A &B)	File, Worm	Stable	March 2001
4	W32/Hybris	Worm	Slight Increase	November 2000
5	W32/Apology (MTX)	File Infector, Trojan	Return to Table	September 2000
6	VBS/Haptime	Script	Slight Decrease	May 2001
7	W32/Funlove	File	Slight Decrease	November 1999
8	VBS/Kakworm	Script	Slight Decrease	December 1999
9	W32/MsInit.worm.a (W32.HLLW.Bymer)	Worm	Return to Table	September 2000
10	VBS/SST (Anna K)	Script, Worm	Return to Table	February 2001

Note: Virus reporting may be weeks behind the first discovery of infection. A total of **201** distinct viruses are currently considered "in the wild" by anti-virus experts, with another **463** viruses suspected. "In the wild" viruses have been reported to anti-virus vendors by their clients and have infected user machines. The additional suspected number is derived from reports by a single source.

FGIU.2642 (DOS Virus): This is a memory-resident DOS virus that infects only .com files.

VBS/Haptime-C (Visual Basic Script Worm): This virus has been reported in the wild. It is a Visual Basic Script worm that spreads via Outlook Express version 5.0. The worm attempts to infect files with the extensions vbs, html, htm, htt and asp. It also attempts to delete exe and dll files when the month plus the day is equal to 13 (for instance, June the 7th).

VBS.Loveletter.CV@mm (Visual Basic Script Worm): This is a Visual Basic Script (VBS) worm that sends e-mail to all contacts that are in the Microsoft Outlook address book. It copies itself into the \Windows\System folder as Msword.vbs and Thwin.vbs, and deletes up to five files with one of the following extensions: .xls, .doc, .wav, .dwg, .mp3, .bak, .wav, .bmp, .htm, .hlp, .chm, .jpg, .gif, .scr, .ttf, .mid, .cdr, .mdb, .dbf, or .ico. The virus saves a list of the files that it deleted in the file \Windows\System\ListWin.txt and also tries to copy itself as A:\Unsch.doc.vbs.

VBS.VBSWG.D@mm (Aliases: I-Worm.Lee.b, VBS/Pica.worm.gen, VBS.Lee@mm) (Visual Basic Script Worm): This is a simple worm that copies itself to the hard disk as C:\Windows\System32\ Independance Day.vbs. It then sends this file to all contacts that are in your Microsoft Outlook address book.

VBS_VBSWG.GEN (Aliases: VBS.Nasara.A@mm, VBS_VBSWG.GEN, VBSWG.GEN, VBSWG.gen@MM, VBS/VBSWG.AF, VBSWG.AF) (Visual Basic Script Worm): This is a worm generated by TROJ_VBSWG_2B. The features of this worm can be determined by the virus writer based on the options in the worm generator console. For example, this worm can be configured to propagate via Microsoft Outlook, by sending itself as an attachment to all addresses listed in an infected user's address book. It can also be configured to replicate via Internet Relay Chat (mIRC) so that it sends copies of itself when the infected user joins a channel. The worm's payload may be configured to display a message box, visit a particular URL, or shut down an infected system.

VCL.Pearl Harbour.959 (DOS Virus): This is an encrypted variant of the DOS virus VCL.Pearl Harbour. The name of the virus is based on its payload. It searches for executables in the root of the drive from which it is executed, and in all subfolders that are contained in the root. When an executable file is found, the virus creates a copy of itself with the same name as the executable file, but with the .com extension. The virus has a payload that is executed on December 7th of any year. The payload displays the following message, for which the virus received its name:

> December 7th, 1941 -- A day that will live in infamy...
> *** REMEMBER PEARL HARBOUR ***

This virus contains a few antidebugging tricks. One of them disables the keyboard. The virus does not re-enable the keyboard after disabling it. Therefore, once the virus has been executed, the keyboard will not work until the computer is restarted.

W32/Hai (Win32 Worm): This worm spreads across local networks, to shared drives with full access enabled. It copies itself to any subdirectory named '\Windows' using a random name and then adds 'run=' to the [Windows] section of the Win.ini configuration file in the subdirectory. The worm is run automatically each time the machine is restarted.

W32/Nimda-B (W32 Executable File Virus): This is a variant of the W32/Nimda-A executable file virus. W32/Nimda-B uses the filenames PUTA!!.SCR and PUTA!!.EML in place of README.EXE and README.EML used by the original W32/Nimda-A. The virus executable file has also been compressed in an apparent attempt to avoid detection by anti-virus products.

W32/Nimda-C (W32 Executable File Virus): This is a variant of the W32/Nimda-A executable file virus. The virus executable file has also been compressed in an apparent attempt to avoid detection by anti-virus products.

W32/Redesi-A (Win32 Worm): This is a Win32 worm, which uses Microsoft Outlook to spread. The worm arrives in an e-mail message with the subject randomly chosen. The body of the message always contains the text "heh. I tell ya this is nuts ! You gotta check it out !." The attached filename is one of the following: redo.exe, si.exe, common.exe, userconf.exe or disk.exe. When the worm is run, it copies itself into C:\rede.exe, C:\si.exe, C:\userconf.exe, C:\common.exe and C:\disk.exe. It then uses Outlook Express to send itself to all contacts found in the address book. Finally, it displays the message box "<filename> is not a valid Win32 application."

W32/Redesi-B (Alias: Win32.Rede.A) (Win32 Worm): This is a worm which uses Microsoft Outlook to spread. The worm arrives in an e-mail message with a subject randomly chosen. The body of the message contains the text:

> "Just received this in my email
> I have contacted Microsoft and they say it's real !
> -----Original Message-----
> From: Microsoft Support Desk [mailto:Support@microsoft.com]
> Subject: Security Update

> Due to the recent spate of email spread computer viruses
> Microsoft Corp has released a security patch.
> Please apply the attached file to your Windows computer
> to stop any future spread or these malicious programs.
> Regards
> Microsoft Support."

The attachment name is randomly chosen from common.exe, rede.exe, si.exe, userconf.exe and disk.exe. When the attachment is run, it displays the message box "Your Windows update has been successful.." The worm copies itself into C:\common.exe, C:\rede.exe, C:\si.exe, C:\userconf.exe and C:\disk.exe. On the 11 November, the worm adds a command to C:\autoexec.bat, which will attempt to format the drive C: on next reboot and display the text "Bide ye the Wiccan laws ye must, In perfect love and perfect trust.." The worm also changes the registry key:

HKLM\Software\Microsoft\Windows\ CurrentVersion\Run\Rede

so that it runs on Windows startup.

W32/Uncensored@MM (Aliases: I-Worm.Desor, TROJ_UNCENSORED.A, W32.Unce@mm, W32/Ducky@mm.90112, Win32.Desor, Win32.HLLW.Hoaxley, Win32/Desor worm) (Win32 Worm): This is a mass-mailing worm written in Visual Basic. When run, it displays a pornographic picture. It then e-mails itself to entries in Outlook's address book.

W97M.Bottra.C (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. It does not have a damaging payload. It exports its virus code to a file in the root of drive C and then imports this code into new host files.

W97M.Grac.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. It creates the file Graciela.src in the Microsoft Word Startup folder.

W97M.Thelar.A (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. It may insert the following text into the currently open document:

- "And Now For Somenthing Completely Different ..."
- "... The Larch..."
- "... The Larch..."
- "... The Larch..."
- "... The Larch..."
- "... The Larch..."
- "... The Larch."

Other than that, this virus does not have a destructive payload.

WM97/Blowup-A (Word 97 Macro Virus): This is a word macro virus that contains a number of anti-Cuban comments. The virus drops a file called info.uue into the root directory of the C: drive. This file contains a uuencoded zip file, info.zip, that itself contains an HTML file called info.htm. The HTML file contains a significant amount of Spanish language text, beginning with the title "Denuncia al gobierno de Cuba," attacking the government of Cuba. The virus makes various changes to the settings in Microsoft Word:

- User name is set to "Halix"
- User initials are set to "HAL"
- User address is set to "Abajo Fidel Castro Ruz"

If the infected user presses ALT+F11 (the key sequence usually used to toggle between Microsoft Word and the Visual Basic Editor), a bogus error message is displayed in a dialog box entitled "Microsoft Word 8.0."

WM97/Marker-GM (Word 97 Macro Virus): This is a corrupted but viable variant of the WM97/Marker-C Word macro virus. Whenever a document is closed, the virus attempts to FTP user information from Word to the Codebreakers site and appends this information to the bottom of the macro as comments.

WM97/Myna-AY (Word 97 Macro Virus): This virus is a member of the WM97/Myna Word macro virus family and contains no malicious payload.

WM97/Myna-AZ (Word 97 Macro Virus): This virus is a variant of the WM97/Myna-J Word macro virus, but contains no malicious payload.

WM97/Myna-BA (Word 97 Macro Virus): This virus is a member of the WM97/Myna Word macro virus family and contains no malicious payload.

WM97/Wrench-R (Word 97 Macro Virus): This is a Microsoft Word macro virus. The virus drops a file called ascii.vxd into the root directory. This file is not viral, but contains the virus code in text form.

Zeton.Mirc (Alias: IRC.Family.gen) (IRC Worm): This is an IRC worm that sends itself using mIRC. It copies itself to the \Windows folder as Notepad.exe and to \Windows\Command as Edit.com, overwriting both files.

Trojans

Trojan Horse programs have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are descriptions of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that their anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
Adshow	N/A	CyberNotes-2001-17
AOL.PWSteal.86016	N/A	CyberNotes-2001-14
Artic	0.6 beta	CyberNotes-2001-14
Asylum	N/A	CyberNotes-2001-18
Backdoor.Bionet.318	N/A	CyberNotes-2001-13
Backdoor.Bionet.40a	N/A	CyberNotes-2001-14
Backdoor.Darkirc	N/A	CyberNotes-2001-15
Backdoor.Darksun	**N/A**	**Current Issue**
Backdoor.Destiny	**N/A**	**Current Issue**
Backdoor.G_Door	N/A	CyberNotes-2001-18
Backdoor.IRC.Critical	N/A	CyberNotes-2001-19
Backdoor.IRC.Flood	N/A	CyberNotes-2001-16
Backdoor.KWM	**N/A**	**Current Issue**
Backdoor.Litmus	**N/A**	**Current Issue**
Backdoor.MiniCommander:	N/A	CyberNotes-2001-16
Backdoor.Penrox	N/A	CyberNotes-2001-17
Backdoor.Slackbot.B	**N/A**	**Current Issue**
Backdoor.SMBRelay	N/A	CyberNotes-2001-10
Backdoor.Teste	N/A	CyberNotes-2001-16
Backdoor.Way	N/A	CyberNotes-2001-18
Backdoor.WLF	N/A	CyberNotes-2001-08
Backdoor-QN	N/A	CyberNotes-2001-13
Backdoor-QO	N/A	CyberNotes-2001-13
Backdoor-QR	N/A	CyberNotes-2001-13
Backdoor-QT	N/A	CyberNotes-2001-14
Backdoor-QV	N/A	CyberNotes-2001-14

Trojan	Version	CyberNotes Issue #
Backdoor-QZ	N/A	CyberNotes-2001-14
BAT.Black	N/A	CyberNotes-2001-11
Bat.FAGE.1482	N/A	CyberNotes-2001-15
Bat.Hexvirus.1414	N/A	CyberNotes-2001-15
Bat.PG94.3964	N/A	CyberNotes-2001-15
BAT.Trojan.DeltreeY	N/A	CyberNotes-2001-07
BAT.Trojan.Tally	N/A	CyberNotes-2001-07
BAT_FORMATC.K	N/A	CyberNotes-2001-13
BioNet	3.13	CyberNotes-2001-07
BSE Trojan	N/A	CyberNotes-2001-07
CodeRed II	II	CyberNotes-2001-16
DMsetup.IRC.Worm	N/A	CyberNotes-2001-13
DonaldD.Trojan.C	N/A	CyberNotes-2001-19
EIC.Trojan	N/A	CyberNotes-2001-14
Eurosol	N/A	CyberNotes-2001-10
Fatal Connections	2.0	CyberNotes-2001-09
Freddy	beta 3	CyberNotes-2001-09
Gift	1.6.13	CyberNotes-2001-09
Goga	N/A	CyberNotes-2001-12
Gribble	N/A	CyberNotes-2001-19
HackTack	N/A	CyberNotes-2001-18
IRC/FinalBot	N/A	CyberNotes-2001-18
Jammer Killah	1.2	CyberNotes-2001-10
JAVA_STORM.A	N/A	CyberNotes-2001-13
JS.Alert.Trojan	N/A	CyberNotes-2001-19
JS.Seeker.B	N/A	CyberNotes-2001-18
JS.StartPage	N/A	CyberNotes-2001-07
JS_EXCEPTION.C	**N/A**	**Current Issue**
JS_OFFENSIVE.A	N/A	CyberNotes-2001-17
JS_ZOPA.A	N/A	CyberNotes-2001-14
KillMBR.g	N/A	CyberNotes-2001-16
Lil Witch FTP	1.0	CyberNotes-2001-19
Noob	4.0	CyberNotes-2001-09
PERL/WSFT-Exploit	N/A	CyberNotes-2001-11
Phoenix	2.1.28	CyberNotes-2001-18
PWS.Cain.dr	N/A	CyberNotes-2001-19
PWSteal.Trojan.D	N/A	CyberNotes-2001-13
QDel172	N/A	CyberNotes-2001-17
Remote Shell Trojan	N/A	CyberNotes-2001-19
SadCase.Trojan	N/A	CyberNotes-2001-09
Scarab	1.2c	CyberNotes-2001-10
SennaSpy Generator	N/A	CyberNotes-2001-13
Septer.Trojan	**N/A**	**Current Issue**
Shake.Trojan	N/A	CyberNotes-2001-20
StealVXS	N/A	CyberNotes-2001-17
Troj/Futs	N/A	CyberNotes-2001-07
Troj/Keylog-C	N/A	CyberNotes-2001-08
Troj/PsychwardB	N/A	CyberNotes-2001-14
Troj/Slack	N/A	CyberNotes-2001-14
Troj/Unite-C	N/A	CyberNotes-2001-09
TROJ_ALLGRO.A	N/A	CyberNotes-2001-17
TROJ_APOST.A	N/A	CyberNotes-2001-18
TROJ_ASIT	N/A	CyberNotes-2001-07
TROJ_BADTRANS.A	N/A	CyberNotes-2001-08
TROJ_BADY	N/A	CyberNotes-2001-15
TROJ_BCKDOR.G2.A	N/A	CyberNotes-2001-11

Trojan	Version	CyberNotes Issue #
TROJ_CAFEIN111.A	N/A	CyberNotes-2001-14
TROJ_CHOKE.A	N/A	CyberNotes-2001-13
TROJ_DSNX.A	N/A	CyberNotes-2001-17
TROJ_EUTH.152	N/A	CyberNotes-2001-08
TROJ_FUNNYFILE.A	N/A	CyberNotes-2001-09
TROJ_HAI.A	N/A	CyberNotes-2001-17
TROJ_HAVOCORE.A	N/A	CyberNotes-2001-09
TROJ_ICMPBOMB.A	N/A	CyberNotes-2001-17
TROJ_IDENTD.B	N/A	CyberNotes-2001-11
TROJ_IE_XPLOIT.A	N/A	CyberNotes-2001-08
TROJ_INCOMM16A.S	N/A	CyberNotes-2001-09
TROJ_INVALID.A	N/A	CyberNotes-2001-18
TROJ_IRC_NETOL.A	N/A	CyberNotes-2001-14
TROJ_JESTRO.A	N/A	CyberNotes-2001-20
TROJ_JOINER.I	N/A	CyberNotes-2001-08
TROJ_KALM.A.SVR	**N/A**	**Current Issue**
TROJ_KEYLOG.25	N/A	CyberNotes-2001-17
TROJ_LASTWORD.A	N/A	CyberNotes-2001-09
TROJ_LATINUS.SVR	N/A	CyberNotes-2001-12
TROJ_LEAVE.A	N/A	CyberNotes-2001-13
TROJ_LINONG.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.A	N/A	CyberNotes-2001-13
TROJ_MADBOX.B	N/A	CyberNotes-2001-13
TROJ_MATCHER.A	N/A	CyberNotes-2001-08
TROJ_MEGA.A	N/A	CyberNotes-2001-12
TROJ_MODNAR.A	N/A	CyberNotes-2001-17
TROJ_MOONPIE.A	N/A	CyberNotes-2001-11
TROJ_MSWORLD.A	N/A	CyberNotes-2001-12
TROJ_MTX.A.DLL	N/A	CyberNotes-2001-09
TROJ_MUSTARD.A	N/A	CyberNotes-2001-19
TROJ_NARCISSUS.A	N/A	CyberNotes-2001-09
TROJ_NEWPIC.A	N/A	CyberNotes-2001-17
TROJ_NEWSAGENT.A	N/A	CyberNotes-2001-16
TROJ_NEWSFLOOD.A	N/A	CyberNotes-2001-13
TROJ_OPTIX.SVR	N/A	CyberNotes-2001-17
TROJ_PICSHOW.A	N/A	CyberNotes-2001-10
TROJ_PSW.GINA.A	N/A	CyberNotes-2001-13
TROJ_RUSH.A	**N/A**	**Current Issue**
TROJ_SCOUT.A	N/A	CyberNotes-2001-08
TROJ_SIRCAM.A	N/A	CyberNotes-2001-15
TROJ_SPYBOY.A	N/A	CyberNotes-2001-18
TROJ_UCON.A	**N/A**	**Current Issue**
TROJ_VAMP.A	N/A	CyberNotes-2001-13
TROJ_VBSWG_2B	N/A	CyberNotes-2001-07
TROJ_VOTE.A	A	CyberNotes-2001-19
TROJ_VOTE.B	B	CyberNotes-2001-20
TROJ_VOTE.C	C	CyberNotes-2001-20
TROJ_WARHOME.A	N/A	CyberNotes-2001-12
TROJ_WHISTLER.A	N/A	CyberNotes-2001-19
TROJ_WINMITE.10	N/A	CyberNotes-2001-08
TROJ_ZERAF.A	N/A	CyberNotes-2001-18
Trojan.Assault.10	10	CyberNotes-2001-15
Trojan.Bat.Live4:	N/A	CyberNotes-2001-16
Trojan.Billrus.Texto	N/A	CyberNotes-2001-14
Trojan.Diagcfg	N/A	CyberNotes-2001-15
Trojan.JS.Clid.gen	N/A	CyberNotes-2001-17

Trojan	Version	CyberNotes Issue #
Trojan.JS.Cover	N/A	CyberNotes-2001-18
Trojan.Lornuke	N/A	CyberNotes-2001-14
Trojan.Offensive	N/A	CyberNotes-2001-17
Trojan.Pounds	N/A	CyberNotes-2001-18
Trojan.PSW.M2.14	N/A	CyberNotes-2001-07
Trojan.Taliban	N/A	CyberNotes-2001-07
Trojan.VBS.PWStroy	N/A	CyberNotes-2001-14
Trojan.VirtualRoot	N/A	CyberNotes-2001-16
Trojan.W32.FireKill	N/A	CyberNotes-2001-07
Trojan.Xtratank	N/A	CyberNotes-2001-17
Trojan.Zeraf	N/A	CyberNotes-2001-17
Trojan.ZeroBoot	N/A	CyberNotes-2001-19
Trojan/PokeVB5	N/A	CyberNotes-2001-07
VBS.AutoExec.Trojan	N/A	CyberNotes-2001-16
VBS.Blank.A	N/A	CyberNotes-2001-14
VBS.Fiber.C	N/A	CyberNotes-2001-18
VBS.Lumorg	N/A	CyberNotes-2001-09
VBS.Masteal.Trojan	**N/A**	**Current Issue**
VBS.Natas	N/A	CyberNotes-2001-16
VBS.Over.Trojan	N/A	CyberNotes-2001-10
VBS.Phybre	N/A	CyberNotes-2001-12
VBS.Reset	N/A	CyberNotes-2001-12
VBS.SystemColor.A	N/A	CyberNotes-2001-11
VBS.Trojan.Icon	N/A	CyberNotes-2001-18
VBS.Trojan.Lariara	N/A	CyberNotes-2001-18
VBS.Zeichen.A	N/A	CyberNotes-2001-08
VBS.Zync.A	N/A	CyberNotes-2001-17
VBS_HAPTIME.A	N/A	CyberNotes-2001-09
VBS_IESTART.A	N/A	CyberNotes-2001-11
W32.BrainProtect	N/A	CyberNotes-2001-07
W32.JavaKiller.Trojan	**N/A**	**Current Issue**
W32.Leave.B.Worm	N/A	CyberNotes-2001-14
W32.Whiter.Trojan	N/A	CyberNotes-2001-20
Y3K Rat	1.6	CyberNotes-2001-11

Backdoor.Darksun: Backdoor.Darksun steals passwords, logs keystrokes, and sends information about your system to a malicious user. It also allows them to remotely control your computer.

Backdoor.Destiny: This is a backdoor Trojan horse. It is a dynamic-link library (DLL) that has extensive control capabilities and allows a malicious user to access the computer.

Backdoor.KWM: This is a Win32 backdoor Trojan that allows a remote host to gain access to an infected computer. There are several known versions of this backdoor, which were distributed as uploads to public Web sites. These EXE and SCR files are Trojan "droppers" that simply drop the actual Trojan program to the Windows directory with the "netcfgh.exe" name, then drop and open a "decoy" file (JPG picture or TXT document). The "decoy" files are created in the C: drive root with the PHOTO.JPG or CONTRACT.TXT names, and then are opened with Explorer. When the actual Trojan file starts, it first of all enables auto dialing by altering the registry key:

HKEY_USERS\.Default\Software\Microsoft\Windows\CurrentVersion\Internet Settings
EnableAutodial

The Trojan then registers itself as a hidden (system) application, then registers itself in the auto-run key in a SYSTEM.INI file (in the Windows directory), sleeps for a short time and runs a main backdoor routine. This routine connects to a host FTP site ftp://ftp.bizland.com/ with a specific name and password, downloads additional EXE components (HEAK.EXE, TEEN1.EXE, TEEN2.EXE, TEEN3.EXE) - which are a keyboard spy (logger), archiver, etc. The Trojan also obtains special CMD files containing instructions written in specific language from this FTP. The backdoor then processes this script file and executes commands that are present here. These commands allow a remote host to operate an infected computer in the following way:

- download files to
- upload files from
- execute local files
- move/copy/delete local files
- upload confidential information to a host FTP (RAS information and cached passwords)

The backdoor also scans disk drives and looks for WebMoney files, and reports them to the host. This allows a host to steal WebMoney information from infected computers. The backdoor also creates the following additional registry keys:

HKLM\Software\Microsoft\Windows\CurrentVersion CmdID = %hostname% ;

where %hostname% is the computer network address SystemNumber = NEW_%system_date% ; where %system_date% is the current date converted to a number and creates additional files in the Windows directory:

Backdoor.Litmus: This is a backdoor Trojan horse that can give a malicious user access to the computer. Like many other backdoor Trojans, Backdoor.Litmus is controlled by the malicious user using IRC channels.

Backdoor.Slackbot.B: Backdoor.Slackbot.B is a backdoor Trojan horse that allows a malicious user to control your computer using Internet Relay Chat (IRC). Backdoor.Slackbot.B can update itself by checking for newer versions over the Internet.

JS_EXCEPTION.C (Aliases: JS.Exception.Exploit, JS.Trojan.Seeker-based): This Trojan has been reported in the wild. This malicious Java Script exploits security vulnerability in a Microsoft Virtual Machine. It allows a Java applet from a malicious Web site to infect a visiting user's machine. This vulnerability allows ActiveX controls to be created and used from a Web page. If a user visits a malicious Web site that exploits this vulnerability, a Java applet on the Web page could run any ActiveX control, even those that are marked as unsafe for scripting. This Java Script uses this vulnerability to change the startup page of Internet Explorer to its desired Web page. It modifies the registry as follows:

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main Start Page = <blocked>

Septer.Trojan: This is a Trojan horse that disguises itself as an appeal for donations from the American Red Cross. If you fill out the form, the Trojan saves the information to a file and then uploads it to a Web site. The Trojan attempts to steal credit card information.

TROJ_KALM.A.SVR (Alias: KALM.A.SVR): This Trojan has been reported in the wild. It is a memory-resident backdoor Trojan allows a remote malicious user access to an infected system. Upon execution, it registers itself as a service process invisible on the task bar (on Windows 9x or Windows ME only). It does not ensure that it is always active in memory, and does not drop any file in the system folders nor modify any system setting such as the registry or the .INI files. It has codes that access the following:

- KERNEL32.EXE
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run Kernel

The above lines of code may copy the Trojan to a KERNEL32.EXE file and create an entry on the Run key of the registry. Bugs in the Trojan program, however cause the above not to execute so that it stays in memory only until the infected computer is restarted. While active, this Trojan opens a TCP port 201, where it listens and waits for commands to execute from a computer where its client program is running. The following text string can be found on the Trojan body: "Kalm."

TROJ_RUSH.A (Aliases: I-WORM.PETIK, RUSH.A): Upon execution, this Trojan creates the following four files:

- a READ_ME.TXT file at the %My Document% folder
- a MAILBOOK.TXT file at the c:\Windows folder
- a MAIL32.EXE file at the c:\Windows\System directory
- a RUSHHOUR.VBS file in the root directory C:\

It sends itself via Microsoft Outlook to all addresses listed in an infected user's address book. It arrives with the attachment ScanVir_25.exe.

TROJ_UCON.A (Aliases: W32/UCON@MM, Win32.Redesi@mm, DarkMachine): This Trojan/worm drops five hidden copies of itself in the C:\ directory as:

- Common.exe
- Rede.exe
- SI.exe
- UserConf.exe
- disk.exe

Using the Windows Messaging APIs or MAPI the Trojan/worm gathers and sends e-mail from, and to, addresses obtained from the infected user's address book. The subject line of the e-mail varies. When the Trojan/worm is run, it displays a message box with the following:

> &ltfilename> is not a valid Win32 application.

Where &ltfilename> is the path and filename of the currently running version of the worm.

W32.JavaKiller.Trojan (Alias: Trojan.W32.JavaKiller):b W32.JavaKiller.Trojan inserts a backdoor Trojan on your system, installs a mIRC client, and creates many files.

VBS.Masteal.Trojan: This is a Trojan horse that is written in the Visual Basic Scripting (VBS) language. When it is executed, the Trojan copies all e-mail address that it finds in the Microsoft Outlook address book to the file C: \Shell.dll.txt. This file is then sent to e-mail addresses that were programmed into the Trojan by the virus writer.